What is claimed is:

1. A system for dynamically identifying internal hosts in a heterogeneous computing environment with multiple subnetworks, comprising:

an analysis module analyzing a plurality of packets, each such packet comprising a source address of an originating host and a destination address of a receiving host; and

a classification module classifying an unknown originating host located at the source address of an outbound packet as an inside host with high confidence, classifying an unknown receiving host located at the destination address of an inbound packet as an inside host, and reclassifying the unknown receiving host as an inside host with high confidence upon receiving a further outbound packet having a source address corresponding to the address of the unknown receiving host.

2. A system according to Claim 1, further comprising:

the classification module further classifying an unknown originating host located at the source address of an inbound packet as an outside host.

3. A system according to Claim 2, further comprising:

the classification module reclassifying the unknown originating host as an inside host with high confidence upon receiving an outbound packet having a source address corresponding to the address of the unknown originating host.

4. A system according to Claim 1, further comprising:

the classification module further classifying an unknown receiving host located at the destination address of an outbound packet as an outside host.

5. A system according to Claim 4, further comprising:

the classification module reclassifying the unknown receiving host as an inside host with high confidence upon receiving an inbound packet having a destination address corresponding to the address of the unknown receiving host.

6. A system according to Claim 1, further comprising:

the classification module maintaining the inside host with high confidence classification of the unknown originating host upon receiving at least one of further inbound packets and further outbound packets.

7. A system according to Claim 1, further comprising:

the classification module maintaining the inside host with high confidence classification of the unknown receiving host upon receiving at least one of further inbound packets and further outbound packets.

8. A system according to Claim 1, further comprising:

the classification module managing packet traffic flow by monitoring the packets and adjusting control flow thereof.

9. A system according to Claim 8, further comprising:

the classification module ignoring packet traffic flow for each packet with an originating host or a receiving host classified as an inside host with high confidence.

10. A system according to Claim 1, wherein the packets are communicated via a point-to-point protocol.

11. A system according to Claim 1, wherein the packets are communicated via an end-to-end protocol.

12. A system according to Claim 1, wherein the packets are communicated via the TCP/IP protocol and each source address and destination address is an internet protocol (IP) address.

13. A method for dynamically identifying internal hosts in a heterogeneous computing environment with multiple subnetworks, comprising:

analyzing a plurality of packets, each such packet comprising a source address of an originating host and a destination address of a receiving host;

classifying an unknown originating host located at the source address of an outbound packet as an inside host with high confidence;

classifying an unknown receiving host located at the destination address of an inbound packet as an inside host; and

reclassifying the unknown receiving host as an inside host with high confidence upon receiving a further outbound packet having a source address corresponding to the address of the unknown receiving host.

14. A method according to Claim 13, further comprising:

classifying an unknown originating host located at the source address of an inbound packet as an outside host.

15. A method according to Claim 14, further comprising:

reclassifying the unknown originating host as an inside host with high confidence upon receiving an outbound packet having a source address corresponding to the address of the unknown originating host.

16. A method according to Claim 13, further comprising:

classifying an unknown receiving host located at the destination address of an outbound packet as an outside host.

17. A method according to Claim 16, further comprising:

reclassifying the unknown receiving host as an inside host with high confidence upon receiving an inbound packet having a destination address corresponding to the address of the unknown receiving host.

18. A method according to Claim 13, further comprising:

maintaining the inside host with high confidence classification of the unknown originating host upon receiving at least one of further inbound packets and further outbound packets.

19. A method according to Claim 13, further comprising:

maintaining the inside host with high confidence classification of the unknown receiving host upon receiving at least one of further inbound packets and further outbound packets.

20. A method according to Claim 13, further comprising:

managing packet traffic flow by monitoring the packets and adjusting control flow thereof.

21. A method according to Claim 20, further comprising:

ignoring packet traffic flow for each packet with an originating host or a receiving host classified as an inside host with high confidence.

22. A method according to Claim 13, wherein the packets are communicated via a point-to-point protocol.

23. A method according to Claim 13, wherein the packets are communicated via an end-to-end protocol.

24. A method according to Claim 13, wherein the packets are communicated via the TCP/IP protocol and each source address and destination address is an internet protocol (IP) address.

25. A computer-readable storage medium holding code for performing the method according to Claims 13, 14, 15, 16, 17, 18, 19, 20 and 21.

26. A system for classifying hosts in a heterogeneous computing environment, comprising:

a table storing records comprising a plurality of states which each specify a location of a host relative to a network domain boundary, the states comprising:

an *Unknown* state describing an undefined host;

an *Outside* state describing a host located outside the network domain boundary;

an *Inside* state describing a host provisionally located inside the network domain boundary; and

an *Inside with High Confidence* state describing a host located inside the network domain boundary;

a traffic manager classifying the hosts based on source address with each outbound packet originating from an *Unknown* state, *Outside* state or *Inside* state into an *Inside with High Confidence* state and classifying the hosts based on destination address with each inbound packet originating from an *Unknown* state or *Outside* state into an *Inside with High Confidence* state.

27. A system according to Claim 26, further comprising:

the traffic manager further classifying the hosts based on source address with each inbound packet originating from an *Unknown* state into an *Outside* state.

28. A system according to Claim 26, further comprising:

the traffic manager passing through packet traffic based on source address with each inbound packet originating from an *Outside* state, *Inside* state or *Inside with High Confidence* state and with each outbound packet originating from an *Inside with High Confidence* state.

29. A system according to Claim 26, further comprising:

the traffic manager further classifying the hosts based on destination address with each outbound packet originating from an *Unknown* state into an *Outside* state.

30. A system according to Claim 26, further comprising:

the traffic manager passing through packet traffic based on destination address with each outbound packet originating from an *Outside* state, *Inside* state or *Inside with High Confidence* state and with each inbound packet originating from an *Inside with High Confidence* state.

31. A system according to Claim 26, further comprising:

the traffic manager ignoring packet traffic based on source address or destination address with each outbound packet and each inbound packet originating from an *Inside with High Confidence* state.

32. A system according to Claim 26, wherein the heterogeneous computing environment is IP compliant.

33. A method for classifying hosts in a heterogeneous computing environment, comprising:

defining a plurality of states which each specify a location of a host relative to a network domain boundary, the states comprising:

an *Unknown* state describing an undefined host;

an *Outside* state describing a host located outside the network domain boundary;

an *Inside* state describing a host provisionally located inside the network domain boundary; and

an *Inside with High Confidence* state describing a host located inside the network domain boundary;

classifying the hosts based on source address with each outbound packet originating from an *Unknown* state, *Outside* state or *Inside* state into an *Inside with High Confidence* state; and

classifying the hosts based on destination address with each inbound packet originating from an *Unknown* state or *Outside* state into an *Inside with High Confidence* state.

34. A method according to Claim 33, further comprising:

classifying the hosts based on source address with each inbound packet originating from an *Unknown* state into an *Outside* state.

35. A method according to Claim 33, further comprising:

passing through packet traffic based on source address with each inbound packet originating from an *Outside* state, *Inside* state or *Inside with High Confidence* state and with each outbound packet originating from an *Inside with High Confidence* state.

36. A method according to Claim 33, further comprising:

classifying the hosts based on destination address with each outbound packet originating from an *Unknown* state into an *Outside* state.

37. A method according to Claim 33, further comprising:

passing through packet traffic based on destination address with each outbound packet originating from an *Outside* state, *Inside* state or *Inside with High Confidence* state and with each inbound packet originating from an *Inside with High Confidence* state.

38. A method according to Claim 33, further comprising:

ignoring packet traffic based on source address or destination address with each outbound packet and each inbound packet originating from an *Inside with High Confidence* state.

39. A method according to Claim 33, wherein the heterogeneous computing environment is IP compliant.

40. A computer-readable storage medium holding code for performing the method according to Claims 33, 34, 35, 36 and 37.